

## REMARKS

Claims 1-10 stand rejected and this rejection is respectively traversed.

To anticipate a claim, the reference must teach every element of the claim. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

To establish a **prima facie** case of **obviousness**, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. In *re* *Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

### Claim 1

Claim 1 has been amended by combination with the features of claim 2 as filed and by specifying that in at least a part of said secure devices, **the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each different chip**. Basis for the latter amendment can be found *inter alia* on page 7, lines 5-7 of the description in the specification as filed. This passage indicates clearly that the invention envisages providing at least a part of a number of secure devices with a unique chip layout. Page 2, line 19 and page 5, lines 22-23 of the description as filed clearly disclose that the secure devices have the same secure functionality, i.e. that the

same algorithms and logic are implemented in them. Thus the amendment does not unduly extend the subject matter of claim 1.

Claim 1 is novel when compared with US 5,898,783, which relates to a system and method to remotely disable a SIM (Subscriber Identity Module) or smart card.

US 5,898,783 does not disclose a number of secure devices, wherein in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each chip. Instead, each SIM card is identified by a unique code and each SIM card is the same in so far as the circuitry layout is concerned (column 5, lines 16-18, wherein the cards are all examples of the card 110 of Figs. 2 and 3).

Claim 1 is novel when compared with US 5,594,657, because US 5,594,657 does not disclose a security system comprising a number of secure devices, much less a number of secure devices wherein in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each different chip. Instead, US 5,594,657 discloses a method of generating a design for implementing a secure device (column 1, line 66 – column 2, line 3).

Claim 1 is novel when compared with US 4,924,075, which relates to a smart IC card provided with data memory that is preferably of the EEPROM type (Electric Erasable Programmable ROM type, see column 3, lines 46-49). US 4,924,075 does not disclose a number of secure devices wherein in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that is

unique to each different chip. Instead, US 4,924,075 discloses a set of secure devices wherein some secure devices are provided with circuitry layout implementing different algorithms and logic (column 7, lines 22-27).

In summary, claim 1 as amended is novel over each of the above-mentioned prior art publications. Accordingly, claim 1 is allowable and, as claims 3 and 5 depend upon claim 1, they are also allowable.

In addition, the subject-manner of amended claim 1 is not derivable in an obvious manner from any of the cited publications, either alone or in combination, as there is no incentive, motivation or suggestion to combine their teachings, and any such combination would not lead to a system falling within the scope of amended claim 1.

US 5,898,783 discloses a security system comprising a number of secure devices, and discloses features provided with the object of discouraging theft and counterfeiting (column 2, lines 8-11). However, as set out above, the known system differs from the one defined in amended claim 1, as it does not have the feature that in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each chip.

The effect of this difference is that, once one prior art chip has been analysed, the layout of all other prior art devices in the system is known. Thus, any security-sensitive information and/or authorisation logic can be extracted from any other prior art secure device by means of a probing attack focussed on the appropriate points in the circuitry

layout. This type of attack is not prevented in the prior art system, so long as a compromised card is not used to identify the user of the SIM card to a telecommunications network. That is to say, in the prior art system, any off-line probing attack remains possible, since a fraudulent card is only disabled when its unique number is found in a disable database (column 4, lines 16-22).

Thus, the objective problem solved by the invention as defined in claim 1 is to provide a security system that protects against a type of attack wherein off-line analysis is used to determine how to extract information from other secure devices in the system.

This problem is solved by the feature of the present invention that in at least a part of said secure devices, **the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each chip.** Thus, knowledge gained through analysis of one secure device cannot be applied by a hacker to extract information from another secure device.

US 5,898,783 does not itself provide a motivation, suggestion or incentive for modification, because it is concerned with preventing straightforward cloning of SIMs (column 2, lines 2-4). This would be adequate where an actual SIM is needed to use an online system. However, it would not prevent analysis of a secure device with a dual functionality, for example as a payment card, with a view to only obtaining all secret banking information from a number of other cards, without using them in a mobile phone first. Thus, the invention provides an enhanced effect not achievable in the system of US 5,898,783.

There is no incentive, motivation or suggestion to combine the teachings of US 5,898,783 with those of US 4,924,075. US 4,924,075 is concerned with the problem of simplifying the operation of a smart card and extending its battery life (column 1, line 60 – column 2, line 6). Thus, starting from US 5,898,783, US 4,924,075 is not an obvious document to consult when faced with the problem outlined above. Even if one were to make a combination, one would not arrive at a security system wherein in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each different chip. This feature is not disclosed in either of the documents (see above).

The combination of US 5,898,783 with US 5,594,657 is not an obvious one either, because US 5,594,357 concerns a method of IC design, in particular the simplification of such a method whilst maintaining a high quality of design (column 2, lines 16-18). Thus, it is in a different field and concerned with a different problem. Furthermore, US 5,594,657 teaches away from claim 1, because the optimiser/compiler disclosed therein will produce an (i.e. *one*) optimised design (column 19, lines 7-10) for subsequent implementation.

In summary, the subject matter of claim 1 is novel and is not rendered obvious by the prior art cited above. Thus, claim 1 meets the conditions for allowance.

Claims 3-5 define a security system with all the features of a security system according to claim 1. For this reason, it is submitted that they too are allowable.

### **Claim 6**

Claim 6 has been amended by combination with the features of claim 7 as filed and by specifying that in at least a part of said secure devices, **the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each different chip**. Basis for the latter amendment can be found *inter alia* on page 7, lines 5-7 of the description in the specification as filed. This passage indicates clearly that the invention envisages providing at least a part of a number of secure devices with a unique chip layout. Page 2, line 19 and page 5, lines 22-23 of the description as filed clearly disclose that the secure devices have the same secure functionality, i.e. that the same algorithms and logic are implemented in them. Thus the amendment does not unduly extend the subject matter of claim 6.

Claim 6 relates to a set of secure devices for a security system according to claim 1 and the set of secure device is distinguished by the fact that, in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each chip. Thus, it is submitted that the subject matter of claim 6 is novel and non-obvious for the same reasons as set out above in relation to claim 1.

### **Claim 8**

Claim 8 has been amended by specifying that, in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that

is unique to each different chip, wherein at least said logic circuitry of the chips of said part of the secure devices is implemented in Field Programmable Gate Array (FPGA) technology, wherein the layout is programmed in the FPGA circuitry in at least one of a volatile and a non-volatile manner. This amendment is based on claim 9 as filed, in so far as the use of FPGA technology is specified. It is further based on the description, page 6, lines 1-14, describing that different chips are implemented with a circuitry layout that is unique to each different chip and at least the logic circuitry is implemented in FPGA technology. Claim 2 of the application as filed provides basis for specifying that a non-volatile manner of programming may be used also.

The subject matter of claim 8 is novel in light of US 5,898,783, which relates to a system and method to remotely disable a SIM (Subscriber Identity Module) or smart card.

US 5,898,783 does not disclose a number of secure devices, **wherein in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each chip.** Instead, each SIM card is identified by a unique code, but is otherwise the same in so far as the circuitry layout is concerned (column 5, lines 16-18, wherein the cards are the cards are all examples of the card 110 of Figs. 2 and 3).

Claim 8 is novel when compared with US 5,594,657, because US 5,594,657 does not disclose a set of secure devices **wherein in at least a part of said secure devices, the same algorithms and logic are implemented in different chips with a circuitry layout that is unique to each different chip.** Instead, US 5,594,657 discloses a method of

generating a design for implementing a secure device (column 1, line 66 – column 2, line 3).

Claim 8 is novel when compared with US 4,924,075, which relates to a smart IC card provided with data memory that is preferably of the EEPROM type (Electric Erasable Programmable ROM type, see column 3, lines 46-49). US 4,924,075 does not disclose a method of manufacturing secure devices for a security system according to claim 1, wherein at least the logic circuitry is implemented in FPGA technology.

Thus, the subject matter of claim 8 is novel.

The method defined in claim 8 does not follow in an obvious manner from the prior art cited, either. Although in principle, none of the above documents relates to a method for manufacturing secure devices, US 5,594,657 comes close by disclosing a method for synthesizing programmable gate array implementations.

US 5,594,657 differs from the invention in that the same algorithms and logic are not implemented in different chips with a circuitry layout that is unique to each different chip. Instead, US 5,594,657 discloses that a compiler/optimiser will produce an (i.e. one) optimised design (column 19, lines 7-10). Although the compiler/optimiser may *evaluate* different circuitry layouts (column 21, lines 3-26), it will then choose only *one* for *implementation* (column 21, lines 33-34: ‘uses the implementation of Fig. 20’). Thus, supplementing the teachings of US 5,594,657 with the usual steps of actually

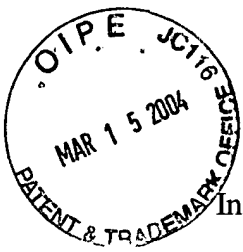


implementing the design produced using the disclosed method, one arrives at a method for manufacturing secure devices with the same (optimised) circuitry layout.

A problem is then that once one chip has been analysed by a hacker, the layout of all other devices in the system is known. Thus, any security-sensitive information and/or authorisation logic can be extracted from any other secure device by means of a probing attack focussed on the appropriate points in the circuitry layout.

US 5,898,783 does not itself provide a motivation, suggestion or incentive for modification of the known method, because it does not concern a method for manufacturing a set of secure devices. Instead, it is concerned with the use of such a set in a telecommunications system. The actual manufacturing can, according to US 5,898,783, use 'conventional processing circuitry' (column 5, lines 35-46). Thus, US 5,898,783 is not an obvious document to consult. Furthermore, US 5,898,783 does not disclose the features distinguishing claim 8 from US 5,594,657, so that a combination of the two teachings could not result in a method according to amended claim 8.

US 4,924,075, relates to a smart IC card provided with data memory that is preferably of the EEPROM type (Electric Erasable Programmable ROM type, see column 3, lines 46-49). US 4,924,075 does not disclose a method of manufacturing secure devices for a security system according to claim 1, wherein at least the logic circuitry is implemented in FPGA technology. It is thus in a completely different field of technology from claim 8.



In summary, the invention defined in claim 8 is not disclosed or rendered obvious by any of the cited prior art references.

**Claims 9-10**

Claims 9 and 10 relate to methods comprising all the features of a method according to amended claim 8, and are thus also considered in a condition for allowance.

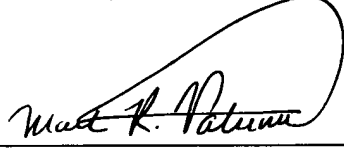
Having tendered the above remarks and amended the claims as indicated herein, Applicant respectfully submits that all rejections have been addressed and that the claims are now in a condition for allowance, which is earnestly solicited.

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due. Furthermore, if an extension is required, then Applicants hereby request such an extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Dated: 3/2, 2004

  
Mark R. Vatuone  
Reg. No. 53,719

12400 Wilshire Blvd.  
Seventh Floor  
Los Angeles, CA 90025-1026  
(408) 947-8200